Amendments to the Specification:

Please amend paragraph 0016 on page 5 as follows:

Referring to Figure 1 there is shown a wireless local area network 10 having a server 12 connected over a wired network 14 to a plurality of access points 16. Network 10 may operate according to a standard protocol, such as IEEE Standard 802.11 to provide wireless network data communications between mobile units 18 and server 12. IEEE Standards 802.11a/b/g are [[is]] fully incorporated herein by reference, and would further be known to one of ordinary skill in the art. As used in this specification, "IEEE Standard 802.11" refers to IEEE Standards 802.11a/b/g.

Please amend line 8 of paragraph 0019 on page 7 as follows:

Some exemplary details of this analysis are now discussed in greater detail. It is noted that, in the following exemplary embodiments of the present invention, the analysis described ~~are~~ is preferably performed by the intrusion detection server 22 using intrusion detection software/firmware.

Please amend lines 16-17 of page 9 (within paragraph 0023) as follows:

in accordance with the invention to store any important variables which pertain to the wireless units on a WLAN such that packets received in the future may be checked against values stored in the state table to detect intrusions and to update the state table as necessary.

Please amend line 1 of page 10 (within paragraph 0024) as follows:

Likewise, the source MAC address may be extracted ~~may be~~ and checked for any suspicious settings – e.g., where the source MAC address is a multicast/broadcast address. An alarm may be similarly triggered in such situations.

Please amend line 7 of paragraph 30 on page 11 as follows:

This check can be performed in numerous ways, including utilizing the IDS keep state to perform the calculation, or checking the direct data frame Duration against its frame length [[)]].

Please amend lines 2-3 of paragraph 0039 on page 13 as follows:

Likewise, illegal authentication frames may indicate network tampering. Authentication sequences may be analyzed to detect such illegal frames, which may be ~~categorizes~~ categorzied as one containing, e.g., an unsupported algorithm number, a wrong authentication sequence number in the sequence (as defined in the 802.11 standard), an unsupported status code, or a wrong DA/SA in the sequence.